IN THE CLAIMS

Please amend the claims as follows:

1. (Withdrawn) A method of implementing token-based electronic security across multiple secure web sites, in which the user has a security token, comprising:

storing unique token identification information, and the seed value of each token, in a security system;

requiring the user, upon login to a secure web site, to enter at least the code generated by the user's token;

passing the user's token code from the web site to the security system;

using the security system to verify whether or not the user's token code was generated by the user's token; and

passing the verification information from the security system to the web site, for use in web site security.

2. (Withdrawn) The method of claim 1 wherein the requiring step further requires the user to enter a user name and user password.

3. (Withdrawn) The method of claim 2 further comprising the step of:

the web site verifying the user name and user password before passing the user's token code to the security system.

4. (Currently Amended) A method of accomplishing two-factor user authentication, comprising:

providing first and second user authentication methods, wherein the first user authentication method is an authentication method selected from authentication methods based on what a user knows and authentication methods based on a characteristic of the user and the second user authentication method is based on a token distributed to the user;

communicating authentication data for both user authentication methods to a first web site using the internet;

authenticating the user at the first web site using the first user authentication method;

if the user is successfully authenticated at the first web site, enabling the communication of token-based authentication data corresponding to the token from the first web site to a second web site using the internet, the authentication data including a token code;

authenticating the user at the second web site based on the token-based authentication data transferred from the first web site;

transmitting results of the authentication at the second web site to the first web site; and

if the authentication at the second web site is unsuccessful, restricting access to sensitive web content on the first web site.

5. (Currently Amended) The method of claim 4, wherein the first web site initially authenticates the user based on the data relating to the first user authentication method.

6-7. (Previously Canceled)

8. (Previously Presented) The method of claim 4, wherein the first web site communicates to the second web site data identifying the user.

9. (Previously Presented) The method of claim 4, wherein the first user authentication method employs a password.

10. (Previously Canceled)

11. (Previously Presented) The method of claim 4, wherein the token is hardware-based, and generates the token code.

12. (Original) The method of claim 11, wherein the token is a stand-alone, portable device.

13. (Original) The method of claim 11, wherein the token is USB-based and is accessed by a browser.

14-15. (Canceled)

16. (Currently Amended) The method of claim 4, wherein ~~one~~ the second user authentication method employs a fixed complex code.

17. (Previously Presented) The method of claim 16, wherein the fixed complex code comprises a one-time password encrypted using a public key infrastructure.

18. (Currently Amended) The method of claim 4, wherein ~~one~~ the second user authentication method is software-based.

19. (Original) The method of claim 4, wherein at least one user authentication method can be used across multiple web sites.

20. (Previously Presented) The method of claim 4, wherein the token is embedded in a cell phone.

21 - 34.(Previously Canceled)

35 - 48.(Canceled)

49. (Currently Amended) A method of adding a second method ~~factor~~ of authentication to a first web site performing ~~having~~ a first ~~factor~~ method of authentication, the method including:

distributing a token to a user;

providing a second website to authorize the user based on the token;

receiving authorization data at the second web site from the first website, the authorization data including user identification data ~~as a function of~~ from the first web site upon the first web site successfully authorizing the user using the first authentication method;

authorizing the user at the second web site based on the token and the user identification data; and

if the authorization at the second website is successful, transmitting data to the first web site indicating the user has been successfully authenticated using at least two ~~factors~~ methods of authentication, wherein the user is granted access to web content on the first web site only if the user has been authenticated using at least two ~~factors~~ methods of authentication.

50. (Currently Amended) A method of adding a second method ~~factor~~ of authentication to a plurality of web sites performing ~~having~~ a first ~~factor~~ method of authentication, the method including::

distributing a token to a user;

providing an authentication web site to authorize the user based on the token;

receiving authorization data from a first web site from the plurality of web sites, the authorization data including user identification data ~~as a function of~~ from the first web site upon the first web site successfully authorizing the user using the first authentication method;

authorizing the user at the authentication web site based on the token and the user identification data; and

if the authorization at the ~~authorization~~ authentication website is successful, transmitting data to the first web site indicating the user has been successfully authenticated using at least two ~~factors~~ methods of authentication, wherein the user is granted access to web content on the plurality of web sites only if the user has been authenticated using at least two ~~factors~~ methods of authentication.